Doc Code: AP.PRE.REQ

PTO/SB/33 (01-09)
Approved for use through 02/28/2009. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)	
80398P252X3	

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____

Signature _____

Typed or printed name _____

Application Number	Filed
10/764,682	2004-01-23

First Named Inventor	
Brant L. Candelore	

Art Unit	Examiner
2434	Yonas A. Bayou

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☑ attorney or agent of record. Registration number 39,018.

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/William W. Schaal/
Signature

William W. Schaal
Typed or printed name

(714) 557-3800
Telephone number

February 17, 2009
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application. No.	:	10/764,682	Confirmation No. 8474
Applicant	:	Brant L. Candelore	
Filed	:	January 23, 2004	
TC/A.U.	:	2434	
Examiner	:	Yonas A. Bayou	
Docket No.	:	80398.P252X3	
Customer No.	:	8791	

Commissioner for Patents
PO Box 1450
Alexandria VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Sir:

In response to the Final Office Action dated November 14, 2008, Applicant would like to request a pre-appeal panel review of the application.

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A mating key gateway adapted to retrieve at least one mating key used to encrypt a program key that is used to scramble digital content prior to transmission to a digital device, comprising:

a bus;

a processor coupled to the bus;

an interface coupled to the bus, the interface being adapted to receive information from (1) a sender of the digital content and (2) either a server controlled by a supplier of the digital device or a trusted third party, the information received by the interface from the sender comprises a mating key generator being a message that comprises an identifier of the supplier; and

a non-volatile storage unit coupled to the bus, the non-volatile storage unit to store a mating key lookup table to identify either the server controlled by the supplier of the digital device or the trusted third party, based on the information received from the sender, from which the at least one mating key is supplied, the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of mating key generators for digital devices supplied by each supplier of a plurality of suppliers including the supplier, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including at least one mating key uniquely corresponding to and formed by at least a portion of one of the mating key generators.

2. (Original) The mating key gateway of claim 1, wherein the interface to receive the information from the sender being one of a cable provider, a satellite-based provider, a terrestrial-based provider, an Internet service provider and a conditional access (CA) provider operating with one of the cable provider, the satellite-based provider, the terrestrial-based provider and the Internet service provider.

3. (Original) The mating key gateway of claim 2, wherein the interface to receive information from the supplier being a manufacturer of the digital device.

4. (Cancelled).

5. (Previously Presented) The mating key gateway of claim 1, wherein the mating key generator received by the interface further comprises an identifier of a provider of a system that enables transmission of both the digital content and the mating key generator to the digital device.

6. (Original) The mating key gateway of claim 5, wherein the mating key generator received by the interface further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the digital content and the mating key generator are transmitted, and (ii) a mating key sequence number.

7. (Original) The mating key gateway of claim 1, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of serial numbers for digital devices supplied by each supplier of a plurality of suppliers including the supplier, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including information to establish communications with a server controlled by one of the plurality of suppliers.

8. (Original) The mating key gateway of claim 1, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of serial numbers for digital devices supplied by each supplier of a plurality of suppliers including the supplier, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including an address to establish communications with a trusted third party authorized by one of the plurality of suppliers.

9. (Previously Presented) The mating key gateway of claim 1, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of mating key generators for digital devices supplied by each supplier of a plurality of suppliers including the supplier and the at least one mating key being formed using at least a portion of one of the mating key generators, and (ii) a second group of entries

corresponding to the first group of entries, each entry of the second group of entries including information to establish communications with a server controlled by one of the plurality of suppliers.

10. (Original) The mating key gateway of claim 9, wherein the information includes an address to establish communications over a network.

11. (Cancelled).

12. (Previously Presented) A mating key gateway adapted to retrieve a mating key used to encrypt a program key that is used to scramble digital content prior to transmission to a digital device, the mating key gateway comprising:

a processor;

an interface in communication with the processor, the interface being adapted to exchange information with (1) a headend and (2) a server configured to store a mating key associated with the digital device; and

a non-volatile storage unit to store a mating key lookup table to identify the server based on the information received from the headend, the information received from the headend includes a mating key generator being a message that comprises an identifier of the manufacturer of the digital device and the mating key being formed using at least a portion of the mating key generator.

13. (Original) The mating key gateway of claim 12, wherein the interface receives the mating key from the server being controlled by a manufacturer of the digital device.

14. (Cancelled).

15. (Previously Presented) The mating key gateway of claim 12, wherein the mating key generator received by the interface further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the digital content and the mating key generator are transmitted, and (ii) a mating key sequence number.

16. (Original) The mating key gateway of claim 12, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range

of serial numbers of digital devices supplied by each of a plurality of manufacturers, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including information to establish communications with a server controlled by one of the plurality of manufacturers.

17. (Original) The mating key gateway of claim 16, wherein the server controlled by one of the plurality of manufacturers is the server.

18. (Previously Presented) The mating key gateway of claim 12, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of mating key generators associated with digital devices supplied by each of a plurality of manufacturers, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including information to establish communications with a server controlled by one of the plurality of manufacturers.

19. (Original) The mating key gateway of claim 18, wherein the information includes an address to establish communications over a network.

20. (Original) The mating key gateway of claim 12 being adapted to additionally store mating keys for selected digital devices.

21. (Previously Presented) A secure content delivery system comprising:

a trusted third party to store a plurality of mating keys associated with digital devices, each mating key being used to encrypt a program key that is used to scramble digital content; and

a mating key gateway in communications with the trusted third party, the mating key gateway to provide information received from a headend to the trusted third party for retrieval of a requested mating key that is computed using the information received from the headend, the information provided to the trusted third party comprises a mating key generator being a message that comprises an identifier of a supplier of one of the digital devices and the mating key generator undergoing a hash operation to produce the requested mating key.

22-23. (Cancelled).

24. (Previously Presented) The secure content delivery system of claim 21, wherein the identifier of the supplier included in the mating key generator identifies a manufacturer of the one of the digital devices.

25. (Previously Presented) The secure content delivery system of claim 21, wherein the mating key generator provided to the trusted third party further comprises an identifier of a provider of the secure content delivery system that enables transmission of both the digital content and the mating key generator to the one of the digital devices.

26. (Previously Presented) The secure content delivery system of claim 21, wherein the mating key generator provided to the trusted third party further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the digital content and the mating key generator are transmitted, and (ii) a mating key sequence number.

27. (Previously Presented) A method comprising:

receiving a mating key generator;

receiving a serial number being used to locate an one-time programmable value;

computing a mating key by performing a computation on the mating key generator and the one-time programmable value to produce the mating key; and

outputting the mating key based on the mating key generator being a message including at least one of (i) a first identifier to identify a manufacturer of the digital device, (ii) a service provider identifier, (iii) a conditional access provider identifier, and (iv) a mating key sequence number and the one-time programmable value being identical to a key stored in a digital device of a set-top box targeted to receive information encrypted with either the mating key or a derivative of the mating key.

28-38. (Cancelled).

REMARKS/ARGUMENTS

Claims 1-3, 5-10, 12, 13, 15-21, and 24-27 are pending in the present application.

This request is in response to the Final Office Action mailed November 14, 2008. In the Final Office Action, the Examiner rejected claims1-3, 5-10, 12, 13, 15-21, and 24-27 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,157,719 (Wasilewski). Applicant respectfully traverses the rejections and contends that the Examiner has not established a *prima facie* case of anticipation.

Pre-appeal panel review of the application in light of the remarks made herein is respectfully requested.

There are several clear errors in the Examiner's rejections and arguments.

1) Wasilewski fails to disclose a mating key lookup table, as recited in claim 1.

Applicant refers to the response filed on August 18, 2008, page 8-9. Among other things, with respect to claims 1, Applicant contends that Examiner failed to identify *the mating key lookup table... comprises (i) a first group of entries forming a range of mating key generators for digital devices supplied by each supplier of a plurality of suppliers including the supplier, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including at least one mating key uniquely corresponding to and partially formed by one of the mating key generators* in Wasilewski.

First, the Examiner alleges that the DHCT 333 of Wasilewski corresponds to the mating key look up table and the EMM corresponds to the mating key generator (Final Office Action, page 5). Applicant respectfully disagrees and submits that the DHCT 333 does not "comprises a first group of entries forming a range of mating key generators…", allegedly the EMMs. In other words, since the EMMS are not stored within the DHCT 333, allegedly the mating key look up table, the DHCT 333 cannot be the mating key lookup table and the EMM cannot be the mating key generator as delineated in claim 1.

Second, the Examiner contends that Wasilewski discloses the mating key lookup table… comprises… (ii) *a second group of entries corresponding to the first group of entries, each entry of the second group of entries including at least one mating key uniquely corresponding to and partially formed by one of the mating key generators* citing col. 25, lines 3-26, as support. For ease of reference, Wasilewski, col. 25, lines 3-26, have been reproduced below:

> "Any one of the public keys for a CAA can be replaced by means of a sequence of two EMMs, the first of which has a sealed digest encrypted with the private key corresponding to a first one of the other two public keys, and the second of which has a sealed digest encrypted with the private key corresponding to the second one of the other two private keys. Each of the two EMMs contains an identifier, the CAAID for the new CAA, a key select value indicating which of the three CAA public keys is to be replaced, and the public key for the new CAA. After the first EMM is successfully authenticated by DHCTSE 627 by verifying the digital signature applied by the first CAA key, DHCTSE 627 computes a MD5 hash of the new CAA public key in this first EMM and stores it. After the second EMM is successfully authenticated by the DHCTSE by verifying the digital signature applied by the second CAA key, the DHCTSE computes a MD5 hash of the new CAA public key included in this second EMM. This second hash is compared with the first. If the hashes are identical, the new CAA public key and CAAID are substituted for the public key and CAAID of the CAA specified by the key select value. A single CAA public key must not be changed twice without one of the other two CAA public keys being changed in between." (Wasilewski, col. 25, lines 3-26)

Applicant respectfully submits that nowhere in this portion or anywhere in Wasilewski discloses the DHCT 333, allegedly the mating key lookup table "comprising … a second group of entries corresponding to the first group of entries…"

Applicant submits that, as discussed above, since the EMM in Wasilewski cannot be the mating key generator, the Examiner has failed to identify a first group of entries and thus, Wasilewski cannot disclose "a second group of entries corresponding to the first group of entries".

Moreover, even assuming that EMMs are the mating key generator, claim 1 delineates "each entry of the second group of entries including at least one mating key uniquely corresponding to and partially formed by one of the mating key generators". *Emphasis Added.* There is no teaching of the EMM "partially forming" any mating keys which are included in the DHCT 333, allegedly the mating key lookup table.

As claimed herein, Applicant respectfully submits that the mating key generator is a specific message construction as explicitly claimed that is used to form the mating key, and clearly, the EMM provided to the DHCT device of Wasilewski is not a mating key generator message and is not used to form mating keys.

Accordingly, Applicant believes that independent claim 1 and claims dependent thereon are in condition for allowance.

2) Wasilewski does not disclose the non-volatile storage unit as recited in claim 12.

Applicant refers to the response filed on August 18, 2008, page 9. Among other things, with respect to claim 12, Applicant contends that the Examiner failed to identify in Wasilewski *a non-volatile storage unit*.

Applicant respectfully submits that the DHCT 333 of Wasilewski does not constitute the non-volatile storage unit as claimed. Herein, Applicant has previously amended claim 12 to include limitations that explicitly recite the mating key being formed using at least a portion of the mating key generator with the "mating key generator" being "a message that comprises an identifier of the manufacturer of the digital device." However, Applicant respectfully submits that the Examiner has mistakenly relied on an improper claim interpretation for the "mating key generator," which is considered by the Examiner to be the EMM (Final Office Action, page 5).

Applicant respectfully submits that the EMM is not configured for use in formulating any mating keys, namely keys used to encrypt a program key. Rather, the EMM is a particular type of message that includes certain information for use in decrypting content. There is no storage of a range of these messages on a supplier basis and the storage of mating keys uniquely corresponding to one of the particular mating key generators and formed with a portion thereof.

Hence, Wasilewski does not teach each and every limitation set forth in independent claim 12. Accordingly, Applicant believes that independent claim 12 and claims dependent thereon are in condition for allowance.

3) Wasilewski does not disclose the mating key generator being a message that comprises an identifier of a supplier of one of the digital devices and the mating key generator undergoing a hash operation to produce the requested mating key, as recited in claim 21.

Applicant refers to the response filed on August 18, 2008, page 10. Among other things, with respect to claim 21, Applicant contends that the Examiner failed to identify in Wasilewski *the mating key generator being a message that comprises an identifier of a supplier of one of the digital devices and the mating key generator undergoing a hash operation to produce the requested mating key*.

Applicant respectfully point out that the Examiner has failed to address the presence or lack of presence of this limitation within Wasilewski (Office Action, page 8) Hence, Applicant respectfully submits that a *prima facie* case of anticipation has not been established.

Accordingly, Applicant believes that independent claim 21 and claims dependent thereon are in condition for allowance.

4) Wasilewski fails to disclose receiving a serial number being used to locate an one-time programmable value, computing a mating key by performing a computation on the mating key generator and the one-time programmable value to produce the mating key, and outputting the mating key based on the mating key generator being a message including at least one of (i) a first identifier to identify a manufacturer of the digital device, (ii) a service provider identifier, [(iii) a conditional access provider identifier,] and (iv) a mating key sequence number…., as recited in claim 27

Applicant refers to the response filed on August 18, 2008, page 10-11. Among other things, with respect to claim 27, Applicant contends that the Examiner failed to identify in Wasilewski "*receiving a serial number being used to locate an one-time programmable value*," "*computing a mating key by performing a computation on the mating key generator and the one-time programmable value to produce the mating key*," and "*outputting the mating key based on the mating key generator being a message including at least one of (i) a first identifier to identify a manufacturer of the digital device, (ii) a service provider identifier, [(iii) a conditional access provider identifier,] and (iv) a mating key sequence number…*"

While the Examiner alleges that the Wasilewski teaches the elements recited above (Final Office Action, page 9), Applicant respectfully disagrees that such teachings are provided by Wasilewski and notes that, for the record, the Examiner already stated that Wasilewski did not feature many of these limitations (*See page 14 of the Office Action mailed October 17, 2007.*).

Moreover, Applicant respectfully submits that Wasilewski fails to describe the above-cited limitations. As an example, for claim 27, the Examiner now alleges that mating key generator is considered to be equivalent to the DHCT private key recited on col. 7, lines 7-11 of Wasilewski. (Final Office Action, page 9) However, the Examiner previously considered an EMM as the mating key generator (Final Office Action, page 5). Applicant respectfully submits that this inconsistent interpretation seemingly supports Applicant's position that the outstanding rejections were and are based on impermissible hindsight reconstruction.

As another example, the serial number of Wasilewski is not used to locate a one-time programmable value. The serial number is provided so that the "demultiplexer 230 can select an

encrypted multi-session key addressed to decoder 240." (Wasilewski, col. 7, lines 9-11). However, the serial number is not used to locate a one-time programmable value as claimed.

Also, Applicant respectfully submits that Wasilewski fails to describe the operation of "computing a mating key by performing a computation on the mating key generator and the one-time programmable value to produce the mating key." The Examiner recites col. 25, lines 4-26 of Wasilewski as support for the teachings of this limitation. However, this recitation is devoid of any computation of a mating key by performing a computation on the mating key generator (DHCT private key) and the one-time programmable value, which has not been explicitly defined by the Examiner.

Hence, Applicant respectfully submits that a *prima facie* case of anticipation has not been established. Therefore, Applicant believes that independent claim 27 and claims dependent thereon are in condition for allowance.

Accordingly, Applicant respectfully requests the Review Panel render a decision allowing the application.

Conclusion

Applicant respectfully requests the Review Panel render a decision allowing the application.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: February 17, 2009

By /William W. Schaal/
William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040